

WHAT IS CLAIMED IS:

- 1 1. A method of handling client state information, said
2 method comprising:
3 receiving, at a first computer system, a first request
4 from a second computer system, wherein the first
5 request is received over a computer network;
6 identifying access control data pertaining to the
7 second computer system;
8 creating an encrypted value based upon the access
9 control data; and
10 storing, on the second computer system, a state
11 management data structure that includes an access
12 control identifier and the encrypted value.
- 1 2. The method of claim 1 further comprising:
2 authenticating a user of the second computer system;
3 and
4 caching, on the first computer system, security
5 attributes of the authenticated user that are too
6 sensitive to be included in the state management data
7 structure, wherein the cached security attributes are
8 indexed by the encrypted value and wherein cached
9 security attributes are adapted to re-establish a
10 security context of the authenticated user.
- 1 3. The method of claim 1 wherein the access control
2 identifier is selected from the group consisting of

3 the access control data and a unique identifier used
4 by the first computer system to map to the access
5 control data stored on an authentication server.

1 4. The method of claim 1 wherein at least one field
2 included in the access control data is selected from
3 the group consisting of: a domain, a maximum age, a
4 path, a port, an authentication strength value, an
5 authenticating server identifier, and an access
6 control privilege identifier.

1 5. The method of claim 1 wherein the creation of the
2 encrypted value further comprises:
3 hashing the access control data using a hashing
4 algorithm, the hashing resulting in a hash value; and
5 encrypting the hash value.

1 6. The method of claim 1 further comprising:
2 storing the encrypted value at the first computer
3 system in response to receiving the first request;
4 receiving a second request from the second computer
5 system;
6 retrieving the state management data structure from
7 the second computer system, the retrieving performed
8 in conjunction with the reception of the second
9 request; and
10 comparing the encrypted value included in the
11 retrieved state management data structure with the
12 encrypted value stored at the first computer system.

1 7. The method of claim 6 further comprising:

2 re-establishing an authenticated user's security
3 context by using the encrypted value as a key to
4 retrieve the access control data cached on the first
5 computer system.

1 8. The method of claim 1 further comprising:

2 authenticating a user of the second computer system,
3 wherein the identifying, creating, and storing are
4 performed in response to successfully authenticating
5 the user.

1 9. The method of claim 8 further comprising:

2 determining that the third computer system does not
3 have access to the authentication data;

4 retrieving the authentication data from an
5 authentication server in response to the
6 determination; and

7 storing the retrieved authentication data on a cache
8 associated with the third computer system.

1 10. The method of claim 1 further comprising:

2 receiving, at the first computer system, a second
3 request from the second computer system;

4 retrieving the state management data structure from
5 the second computer system, the retrieving performed
6 in conjunction with the reception of the second
7 request;

8 determining that the retrieved state management data
9 structure is stale based on a timestamp included in
10 the state management data structure; and

11 authenticating a user of the second computer system in
12 response to the determination.

1 11. An first information handling system comprising:

2 one or more processors;

3 a memory accessible by the processors;

4 a network interface connecting the information
5 handling system to a computer network;

6 a tool for handling client state information, the tool
7 including software effective to:

8 receive, at the first information handling
9 system, a first request from a second information
10 handling system, wherein the first request is
11 received over a computer network;

12 identify access control data pertaining to the
13 second information handling system;

14 create an encrypted value based upon the access
15 control data; and

16 store, on the second information handling system,
17 a state management data structure that includes
18 an access control identifier and the encrypted
19 value.

1 12. The information handling system of claim 11 further
2 comprising software effective to:

3 authenticate a user of the second information handling
4 system; and

5 cache, on the first information handling system,
6 security attributes of the authenticated user that are
7 too sensitive to be included in the state management
8 data structure, wherein the cached security attributes
9 are indexed by the encrypted value and wherein cached
10 security attributes are adapted to re-establish a
11 security context of the authenticated user.

1 13. The information handling system of claim 11 wherein
2 the access control identifier is selected from the
3 group consisting of the access control data and a
4 unique identifier used by the first information
5 handling system to map to the access control data
6 stored on an authentication server.

1 14. The information handling system of claim 11 wherein at
2 least one field included in the access control data is
3 selected from the group consisting of: a domain, a
4 maximum age, a path, a port, an authentication
5 strength value, an authenticating server identifier,
6 and an access control privilege identifier.

1 15. The information handling system of claim 11 wherein
2 the creation of the encrypted value further comprises
3 software effective to:

4 hash the access control data using a hashing
5 algorithm, the hashing resulting in a hash value; and
6 encrypt the hash value.

1 16. The information handling system of claim 11 further
2 comprising software effective to:
3 store the encrypted value at the first information
4 handling system in response to receiving the first
5 request;
6 receive a second request from the second information
7 handling system;
8 retrieve the state management data structure from the
9 second information handling system, the retrieval
10 performed in conjunction with the reception of the
11 second request; and
12 compare the encrypted value included in the retrieved
13 state management data structure with the encrypted
14 value stored at the first information handling system.

1 17. The information handling system of claim 16 further
2 comprising software effective to:
3 re-establish an authenticated user's security context
4 by using the encrypted value as a key to retrieve the
5 access control data cached on the first information
6 handling system.

1 18. The information handling system of claim 11 further
2 comprising software effective to:
3 authenticate a user of the second information handling
4 system, wherein the identifying, creating, and storing
5 are performed in response to successfully
6 authenticating the user.

1 19. The information handling system of claim 18 further
2 comprising software effective to:
3 determine that a third information handling system
4 does not have access to the authentication data;
5 retrieve the authentication data from an
6 authentication server in response to the
7 determination; and
8 store the retrieved authentication data on a cache
9 associated with the third information handling system.

1 20. The information handling system of claim 11 further
2 comprising software effective to:
3 receive, at the first information handling system, a
4 second request from the second information handling
5 system;
6 retrieve the state management data structure from the
7 second information handling system, the retrieving
8 performed in conjunction with the reception of the
9 second request;
10 determine that the retrieved state management data
11 structure is stale based on a timestamp included in
12 the state management data structure; and
13 authenticate a user of the second information handling
14 system in response to the determination.

1 21. A computer program product stored on a computer
2 operable media for handling client state data, said
3 computer program product comprising:

4 means for receiving, at a first computer system, a
5 first request from a second computer system, wherein
6 the first request is received over a computer network;
7 means for identifying access control data pertaining
8 to the second computer system;
9 means for creating an encrypted value based upon the
10 access control data; and
11 means for storing, on the second computer system, a
12 state management data structure that includes an
13 access control identifier and the encrypted value.

1 22. The computer program product of claim 21 further
2 comprising:
3 means for authenticating a user of the second computer
4 system; and
5 means for caching, on the first computer system,
6 security attributes of the authenticated user that are
7 too sensitive to be included in the state management
8 data structure, wherein the cached security attributes
9 are indexed by the encrypted value and wherein cached
10 security attributes are adapted to re-establish a
11 security context of the authenticated user.

1 23. The computer program product of claim 21 wherein the
2 access control identifier is selected from the group
3 consisting of the access control data and a unique
4 identifier used by the first computer system to map to
5 the access control data stored on an authentication
6 server.

1 24. The computer program product of claim 21 wherein at
2 least one field included in the access control data is
3 selected from the group consisting of: a domain, a
4 maximum age, a path, a port, an authentication
5 strength value, an authenticating server identifier,
6 and an access control privilege identifier.

1 25. The computer program product of claim 21 wherein the
2 means for creating the encrypted value further
3 comprises:

4 means for hashing the access control data using a
5 hashing algorithm, the hashing resulting in a hash
6 value; and

7 means for encrypting the hash value.

1 26. The computer program product of claim 21 further
2 comprising:

3 means for storing the encrypted value at the first
4 computer system in response to receiving the first
5 request;

6 means for receiving a second request from the second
7 computer system;

8 means for retrieving the state management data
9 structure from the second computer system, the means
10 for retrieving performed in conjunction with the
11 reception of the second request; and

12 means for comparing the encrypted value included in
13 the retrieved state management data structure with the
14 encrypted value stored at the first computer system.

1 27. The computer program product of claim 26 further
2 comprising:

3 means for re-establishing an authenticated user's
4 security context by using the encrypted value as a key
5 to retrieve the access control data cached on the
6 first computer system.

1 28. The computer program product of claim 21 further
2 comprising:

3 means for authenticating a user of the second computer
4 system, wherein the identifying, creating, and storing
5 are performed in response to successfully
6 authenticating the user.

1 29. The computer program product of claim 28 further
2 comprising:

3 means for determining that the third computer system
4 does not have access to the authentication data;

5 means for retrieving the authentication data from an
6 authentication server in response to the
7 determination; and

8 means for storing the retrieved authentication data on
9 a cache associated with the third computer system.

1 30. The computer program product of claim 21 further
2 comprising:

3 means for receiving, at the first computer system, a
4 second request from the second computer system;

5 means for retrieving the state management data
6 structure from the second computer system, the means
7 for retrieving performed in conjunction with the
8 reception of the second request;

9 means for determining that the retrieved state
10 management data structure is stale based on a
11 timestamp included in the state management data
12 structure; and

13 means for authenticating a user of the second computer
14 system in response to the determination.